

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Інв. № ориг.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

**Центр сертифікації ключів
ринку електричної енергії**

Комплексна система захисту інформації.
Комплекс засобів захисту

Опис програмного забезпечення

ЄААД.468244.185.ПА.02

ЗМІСТ

1 СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	4
2 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ	5
2.1 КЗЗ операційної системи з лінійки Windows	5
2.1.1 Забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК.....	5
2.1.2 Забезпечення безперервності функціонування ОС	5
2.1.3 Ведення журналів аудиту.....	6
2.1.4 Забезпечення можливості адміністрування, керування і підтримки ОС	6
2.2 КЗЗ СКБД Microsoft SQL Server 2012	6
2.2.1 Керування безпекою сервера БД на основі ролей.....	6
2.2.2 Права доступу, що реалізуються штатним КЗЗ сервера БД.....	8
2.2.3 Інші засоби штатних КЗЗ сервера БД	9
2.3 КЗЗ СКБД MySql.....	9
2.3.1 Права доступу, що реалізуються штатним КЗЗ	10
2.3.2 Інші засоби штатних КЗЗ сервера БД	10
2.4 КЗЗ HTTP-сервера Apache	11
2.4.1 Категорії інформації, що обробляється веб-сервером.....	11
2.4.2 Методи обробки інформації веб-сервера.....	11
2.4.3 Основні функції штатного КЗЗ веб-сервера	11
2.5 Підсистема антивірусного захисту	13
2.5.1 Застосування евристичних методів захисту у процесі викриття шкідливого ПЗ.....	13
2.5.2 Захист файлової системи	13
2.5.3 Оновлення антивірусних баз	14
2.6 КЗЗ операційної системи з лінійки Linux для серверів.....	14
2.6.1 Забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК.....	14
2.6.2 Забезпечення безперервності функціонування ОС	14
2.1.3 Ведення журналів аудиту.....	14
2.1.4 Забезпечення можливості адміністрування, керування і підтримки ОС	15

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ЕОМ	- Електронно-обчислювальна машина
ЕОТ	- Електронно-обчислювальна техніка
ЕЦП	- Електронний цифровий підпис
ЗТМ	- Зовнішні телекомунікаційні мережі
ІТС	- Інформаційно-телекомунікаційна система
КЗЗ	- Комплекс засобів захисту
КЗІ	- Криптографічний захист інформації
КТЗ	- Комплекс технічних засобів
КСЗІ	- Комплексна система захисту інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
НКІ	- Носій ключової інформації
ОС	- Операційна система
ПЗ	- Програмне забезпечення
РС	- Робоча станція
СКБД	- Система керування базами даних
ЦСК	- Центр сертифікації ключів
HTTP	- Hyper Text Transfer Protocol
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)

1 СТРУКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Структура програмного забезпечення (ПЗ) комплексу засобів захисту (КЗЗ) наводиться за принципом цільового використання.

Опис КТЗ КЗЗ наведено у документі ЄААД.468244.185.П9.02.

Прив'язка до конкретних засобів ЦСК та опис комплексної системи захисту інформації (КСІ) наведено у загальному описі системи (документ ЄААД.468244.185.ПД.02).

До складу програмного забезпечення КЗЗ входить:

- КЗЗ операційної системи (далі - ОС) з лінійки Windows для PC;
- КЗЗ операційної системи з лінійки Windows для серверів;
- КЗЗ операційної системи з лінійки Linux для серверів;
- КЗЗ серверів, що складається з:
 - КЗЗ ПК центральних серверів;
 - КЗЗ ПК серверів взаємодії;
 - КЗЗ СКБД Microsoft SQL;
 - КЗЗ ПЗ LDAP-серверу;
 - КЗЗ СКБД MySQL;
 - КЗЗ HTTP-сервера Apache.
- КЗЗ ПЗ моніторингу;
- КЗЗ ПК PC генерації ключів;
- КЗЗ ПЗ користувача ЦСК;
- підсистема антивірусного захисту.

2 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ

2.1 КЗЗ операційної системи з лінійки Windows

Робочі станції та сервер застосовувать приймають участь у процесах з обробки інформації. В якості ОС робочих станцій використовується MS Windows 8.1 Enterprise, у якості ОС серверів використовується MS Windows Server 2012 R2 Standard. Так як MS Windows 8.1 Enterprise, MS Windows Server 2012 R2 реалізують ідентичні механізми захисту, далі під ОС будуть матися на увазі операційні системи MS Windows 8.1 Enterprise та MS Windows Server 2012 R2 Standard.

КЗЗ ОС реалізує такі функції:

- забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК, що зберігаються у файловій системі PC;
- забезпечення безперервності функціонування ОС;
- ведення журналів аудиту;
- забезпечення можливості адміністрування, керування і підтримки ОС.

2.1.1 Забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК

Операційна система (ОС) надає доступ до своїх ресурсів тільки авторизованим користувачам. Список доступу включає перелік користувачів, яким дозволено доступ до об'єкта, а також набір дозволених над об'єктом дій, що у явному вигляді є елементами захисту від НСД.

Для спрощення керуванням доступом до об'єктів і захисту від НСД, ОС дозволяє створювати групи безпеки, дозволяючи призначати дозволи і права для групи користувачів, а не окремого облікового запису користувача. Для надання доступу до ресурсів, обліковий запис може бути добавлений або видалений з групи користувачів. Після інсталяції ОС в ньому створюються вбудовані групи, які дають право на виконання напередвизначених системних завдань.

Для додаткового захисту від НСД файли системи можуть шифруватися прозорим для користувача способом за допомогою ключа, який генерується випадковим чином. ОС дозволяє забезпечити доступ до цих файлів декільком користувачам.

За допомогою політик обмеженого використання в ОС реалізується спосіб ізоляції підозрілого, потенційно небезпечного коду, завдяки якому забезпечується захист комп'ютера від вірусів, "троянських коней" і "червів". Ці політики надають користувачу можливість обрати спосіб, за допомогою якого він буде здійснювати керування програмними продуктами на своєму комп'ютері. Програмний продукт може керуватися "жорстко" (адміністратор сам вирішує, яким чином, коли і де буде здійснюватися виконання коду) або взагалі не керуватися (виконання конкретного коду заборонено), що може повністю заборонити несанкціонований доступ до об'єктів у файловій системі.

2.1.2 Забезпечення безперервності функціонування ОС

Важливим, а іноді необхідним для роботи ОС є забезпечення безперервності функціонування. Невиконання цієї умови може привести до втрати важливої інформації. Головними умовами безперервного функціонування є контроль виходу із ладу компонентів системи, що може привести до завершення роботи ОС, і, у випадку виходу, мати можливість швидкого відновлення робочого стану.

До складу ОС входить моніторинг завершення роботи, який забезпечує механізм детального документування причин відключення і перезапуску комп'ютера. Ці дані використовуються для аналізу причин аварійного завершення роботи комп'ютера і більш повного аналізу системного середовища.

У ОС входять стандартні засоби запобігання втраті даних і їхньому відновленню. Програма архівації і системні засоби надають користувачам можливість виконувати архівування файлів і папок на незмінні або змінні пристрої збереження. Одним з ефективних варіантів застосування цих засобів архівації є налагодження їх для регулярної архівації локальних файлів на сервері, дані з якого згодом архівуються відповідно до порядку, прийнятому в організації.

Засоби перевірки драйверів пристроїв забезпечують можливість встановлення тільки тих драйверів, що пройшли відповідні випробування для підтвердження якості. Відкат драйверів дозволяє повернути ОС в попередній стан після невдалого встановлення драйверу. Дана можливість сприяє забезпеченню надійності роботи (стійкості) системи.

Функціональна можливість відновлення системи дозволяє повертати комп'ютер у той стан, в якому він знаходився до виникнення проблеми. При цьому не відбувається втрати особистих файлів даних, що можуть містити, наприклад, документи. При використанні даної можливості здійснюється активний

моніторинг змін системних характеристик і деяких файлів застосувань, а також автоматичне створення контрольних точок відновлення.

2.1.3 Ведення журналів аудиту

В ОС присутній набір засобів аудиту, призначених для моніторингу та виявлення умов і подій що пов'язані з можливим НСД або є небажаними, які виникають в обчислювальному середовищі. Моніторинг системних подій дозволяє виявляти порушників, що здійснюють спроби НСД, а також фіксувати спроби НСД з метою фальсифікації та видалення даних, які знаходяться на локальному комп'ютері.

При аудиті, частіше за все, реєструються такі події як доступ до об'єктів, керування групами користувачів і обліковими записами груп, а також вхід користувачів в систему і вихід з неї. Аудит дозволяє вести моніторинг конкретних подій, наприклад, неуспішних спроб входу до системи. Перегляд журналу безпеки виконується за допомогою засобів перегляду подій. Політика аудиту дозволяє визначати події, для яких повинен проводитися аудит.

2.1.4 Забезпечення можливості адміністрування, керування і підтримки ОС

Операційна система Windows володіє багатьма можливостями адміністрування, керування та підтримки. Системи адміністрування надають можливість керувати файловою системою, установкою та видаленням програмного забезпечення, налаштування журналів безпеки та багато інших.

ОС має кілька оснасток для керування і адміністрування локального та віддалених комп'ютерів. Оснастка «Керування комп'ютером» поєднує кілька засобів адміністрування ОС в одне дерево консолі, що забезпечує легкий доступ до властивостей адміністрування конкретного комп'ютера.

Перегляд подій системи використовується для перегляду і керування журналами системних і програмних подій, а також подій безпеки на комп'ютері. У вікні перегляду подій збираються відомості про несправності устаткування і неполадки програмного забезпечення, а також відображаються події безпеки.

Оснастка "Локальна політика безпеки" дозволяє налаштовувати параметри безпеки локального комп'ютера. За допомогою неї можливо налаштувати політику паролів, політику облікових записів, політику аудиту, політику безпеки IP, визначення прав користувачів, призначення агентів відновлення зашифрованих даних. Якщо комп'ютер є членом домену, ці параметри можуть бути перевизначені в політиках, отриманих з домену.

ОС має системну службу, яка дозволяє коректно встановлювати, налагоджувати, відслідковувати та видаляти програмне забезпечення (ПЗ). Це дозволяє мінімізувати час простою системи, підвищити її стабільність та безпеку.

Консоль керування дозволяє зберігати і відкривати оснастки адміністрування (консолей MMC), які керують устаткуванням, програмними і мережними компонентами ОС.

Майстер переміщення файлів і конфігурації дозволяє переносити робочі і конфігураційні файли користувача з однієї робочої станції на іншу шляхом виконання інструкцій. Майстер дозволяє вибрати призначені для переносу файли, їхні типи і папки. Підтримується також перенос настроювань для обмеженого набору застосувань, включаючи застосування Microsoft Office.

Функція швидкого переключення користувачів дозволяє декільком особам працювати з комп'ютером так, ніби він належить кожному з них. Немає необхідності забезпечувати вихід із системи іншого користувача або зберігати його файли. Замість цього в ОС застосовується технологія служби терміналів для запуску унікальних сеансів користувачів, що дозволяє цілком розділити дані різних користувачів. Якщо застосовуються паролі користувачів, ці сеанси є взаємно безпечними.

Центр довідки та підтримки об'єднує відповідні функції ОС, що підвищує доступність документації та допомоги. ОС забезпечує підтримку діагностування та усунення неполадок користувачем системи.

ОС надає можливість віддаленого керування ОС спільно з іншим користувачем, комп'ютер якого підключений до мережі. Адміністратор може бачити екран користувача зі свого комп'ютеру і допомагати в усуненні технічних неполадок за допомогою своєї клавіатури та «миші».

З дозволу користувача, ОС завантажує критично важливі оновлення з Інтернету в фоновому режимі. Завантаження не потребує від користувача додаткових зусиль або переривання в роботі.

2.2 КЗЗ СКБД Microsoft SQL Server 2012

У якості серверу БД у КЗІ використовується MS SQL Server 2012. Штатний КЗЗ сервера БД MS SQL Server 2012 є інтегрованим з КЗЗ операційних систем.

2.2.1 Керування безпекою сервера БД на основі ролей

На рівні сервера система безпеки оперує такими поняттями:

- автентифікація;
- обліковий запис;
- вбудовані ролі сервера.

Кожному користувачу присвоюється обліковий запис з визначеними правами. Автентифікація користувачів проводиться або за обліковим записом ОС MS Windows 8.1 Enterprise/Server 2012, або в змішаному режимі - за обліковим записом ОС або обліковим записом на рівні сервера. Тобто система аутентифікації MS SQL Server 2012 використовує системні механізми щоб підвищити рівень безпеки. Паролі користувачів та інші дані про них зберігаються на сервері в системній базі даних Master в таблиці SysLogins. Паролі можуть зберігатися як в зашифрованому, так і в незашифрованому, але спеціально перетвореному вигляді. При інсталяції сервера автоматично створюється обліковий запис системного адміністратора сервера sa, пароль до якого не можна залишати пустим. Облікові записи користувачів організовані в ролі (аналог груп в лінійці ОС Windows NT), набір яких є фіксованим. Нижче наведено список ролей сервера.

На рівні бази даних використовуються поняття:

- користувач бази даних;
- фіксована роль бази даних;
- користувацька роль бази даних;
- роль застосування.

Таблиця 2.1 Вбудовані ролі сервера

Вбудована роль сервера	Опис прав членів ролі
sysadmin	Мають абсолютні права в SQL Server 2012.
setupadmin	Права по керуванню зв'язаними серверами, конфігуруванню процедур, що зберігаються, які запускаються на старті SQL Server 2012, право додавати облікові записи в роль setupadmin .
serveradmin	Право на зупинку сервера, зміну параметрів роботи служб, застосування змін, керування повнотекстовим пошуком. Зазвичай використовується користувачами, які виконують адміністрування сервера.
securityadmin	Можливість створювати нові облікові записи, надавати їм права на створення БД та їх об'єктів, керувати зв'язаними серверами, включати облікові записи в роль securityadmin, читати журнал помилок SQL Server.
processadmin	Керування процесами, які реалізує SQL Server 2012, тобто виконання команди KILL. Право включати облікові записи в роль processadmin.
dbcreator	Право створювати нові БД, видаляти або перейменовувати вже існуючі, відновлювати БД з резервних копій
bulkadmin	Право вставляти дані з допомогою засобів масової зачатки без безпосереднього доступу до таблиць

У MS SQL Server 2012 автоматично створюються два користувача.

- Власник БД (dbo). Власник БД має абсолютні права з керування нею. За замовчуванням в користувача dbo відображається обліковий запис sa, якому тим самим надаються максимальні права в базі даних. Крім того, всі члени цієї ролі вважаються власниками БД. Користувач dbo включений до ролі db_owner і не може бути видалений з неї.
- Гість (guest). Якщо обліковому запису явно не надано доступ до БД, то вона автоматично відображається сервером в користувача guest. За допомогою цього облікового запису можливо надавати права на доступ до об'єктів БД, що необхідні кожному користувачу. Дозволивши доступ користувачу guest, адміністратор, тим самим, надає аналогічні права доступу всім обліковим записам, заведеним на SQL Server 2012. Для підвищення безпеки інформації, що зберігається в БД, рекомендовано видалити користувача guest з бази даних.

Для вирішення стандартних задач з розмежування прав доступу використовуються фіксовані ролі БД. Крім того в КЗЗ сервера БД реалізовано можливість створювати роль користувача із заданими правами.

Таблиця 2.2 Фіксовані ролі БД

Найменування ролі	Стислий опис
db_securityadmin	Члени ролі можуть керувати правами доступу до об'єктів БД інших користувачів та їх членством в інших ролях

db_owner	Члени ролі мають права власника, тобто можуть виконувати довільні дії
db_denydatawriter	Членам цієї ролі заборонено змінювати дані незалежно від виданих дозволів
db_denydatareader	Членам цієї ролі заборонено читати дані незалежно від виданих дозволів
db_ddladmin	Члени ролі можуть створювати, змінювати і видаляти об'єкти БД
db_datawriter	Члени ролі можуть змінювати дані в будь-якій таблиці і наданій БД
db_datareader	Члени ролі можуть читати дані з будь-яких таблиць і наданій БД
db_backupoperator	Члени ролі виконують резервне копіювання бази даних
db_accessadmin	Члени ролі мають право керувати користувачами БД: створювати, видаляти і змінювати.

Ролі застосувань дозволяють налаштувати однакові права для великої кількості користувачів. При цьому відповідальність за автентифікацію користувача, який користується застосуванням покладається на саме застосування. Для MS SQL Server 2012 вважається достатнім, щоб був пред'явлений пароль, який відповідає ролі. Пароль може вводитися користувачем або зберігатися у застосуванні.

2.2.2 Права доступу, що реалізуються штатним КЗЗ сервера БД

Усі існуючі в БД права доступу розбиваються на три класи:

- права доступу до даних;
- права на виконання процедур, що зберігаються;
- права на виконання команд Transact-SQL.

2.2.2.1 Права доступу до даних

Право «INSERT» дозволяє вставляти в таблицю або в подання. Як наслідок, право INSERT може бути видано тільки на рівні таблиці або подання, і не може бути надане на рівні стовпця.

Право «UPDATE» видається або на рівні таблиці, або на рівні стовпця.

Право «DELETE» дозволяє видаляти рядки з таблиці або подання. Як і право INSERT, право DELETE може бути видано тільки на рівні таблиці або подання і не може бути видано на рівні стовпця.

Право «SELECT» дозволяє здійснювати вибірку даних. Може видаватися як на рівні таблиці, так и на рівні окремого стовпця.

Право «REFERENCES» надає можливість посилатися на вказаний об'єкт. Відносно таблиць дозволяє користувачу створювати зовнішні ключі, які посилаються на первинний ключ або унікальний стовбець цієї таблиці. Відносно подання право REFERENCES дозволяє зв'язувати їх зі схемами таблиць, на підставі яких, створюються ці подання. Це дає можливість відслідковувати зміни структури вихідних таблиць, які можуть вплинути на роботу подання..

2.2.2.2 Права на виконання процедур і функцій, що зберігаються

Єдине право доступу, яке може бути надано відносно процедури, що зберігається - це право на її виконання (EXECUTE). Крім того, власнику процедури, що зберігається, дозволяється продивлятися та змінювати її код.

2.2.2.3 Права на виконання команд Transact-SQL.

Права на виконання команд Transact-SQL призначено для керування можливостями користувача створювати нові об'єкти БД.

Право «CREATE DATABASE» дозволяє створювати бази даних.

Право «CREATE TABLE» дозволяє створювати таблиці.

Право «CREATE VIEW» дозволяє створювати подання.

Право «CREATE PROCEDURE» дозволяє створювати процедури, що зберігаються.

Право «CREATE FUNCTION» дозволяє створювати функції користувачів.

Право «CREATE RULE» дозволяє створювати правило.

Право «CREATE DEFAULT» дозволяє створювати значення за замовчуванням.

Право «BACKUP DATABASE» дозволяє створювати резервну копію БД.

Право «BACKUP LOG» дозволяє створювати резервну копію журналу транзакцій.

Право «ALL» надає можливість користуватися усіма вище переліченими правами.

Члени вбудованої ролі сервера «sysadmin» та вбудованої ролі БД «dbowner» автоматично мають право ALL. Члени інших вбудованих ролей мають набір прав, відповідно до функцій ролі.

2.2.3 Інші засоби штатних K33 сервера БД

До інших засобів штатних K33 сервера БД слід віднести:

- шифрування об'єктів БД;
- заборона доступу до об'єктів БД;
- засоби аудиту.

Додатковим засобом захисту інформації є використання вбудованих засобів шифрування об'єктів БД. Щоб зашифрувати об'єкт, при його створенні необхідно вказати опцію «WITH ENCRYPTION».

Штатні K33 сервера БД дозволяють встановлювати два типи заборони доступу: явна та неявна. Різниця між ними в тому, що у разі явної заборони користувач не отримає доступу до об'єкту БД ні за яких умов. За неявної заборони користувач може отримати доступ до об'єкту БД. Наприклад у випадку, якщо користувач має неявну заборону на доступ, але його ролі надано явний дозвіл, то він отримає доступ. І навпаки, якщо ролі користувача неявно заборонено доступ, але користувач має явний дозвіл, то він також отримає доступ до об'єкту БД.

У MS SQL Server 2012 реалізовано засоби аудита. Для налаштування засобів аудиту необхідно визначити які спроби доступу слід відслідковувати:

Опція «None» вказує на непотрібність протоколювати спроби доступу користувачів до БД.

Опція «Success» визначає, що сервер БД має записувати до журналу тільки ті спроби реєстрації, які завершилися вдало. У цьому випадку журнал міститиме перелік усіх користувачів, які працювали з даними сервера БД.

Опція «Failure» вказує на необхідність відслідковувати тільки невдалі спроби отримання доступу. Це дозволяє виявити спроби злому системи шляхом підбору паролів.

Опція «All» визначає режим в якому сервер БД зберігає інформацію як про вдалі, так і про невдалі спроби отримання доступу.

Інформація системи аудита в залежності від конфігурації сервера зберігається або в журналі застосувань ОС, або в журналі помилок БД (error log), або в обох одразу. Рекомендується використання журналу застосувань ОС, оскільки при видаленні інформації з цього журналу залишається запис про дату і час очистки журналу. Наявність такого запису без відповідного акту копіювання вмісту і очистки журналу є підставою для розслідування діяльності адміністратора.

2.3 K33 СКБД MySql

У якості серверу БД у K3I використовується MySQL Server. K33 СКБД призначена для:

- керування безпекою сервера БД на основі облікових записів;
- розмежування прав доступу на виконання команд SQL да виконання процедур, що зберігаються;
- забезпечення шифрування об'єктів БД;
- забезпечення заборони доступу до об'єктів БД;

На рівні сервера система безпеки оперує такими поняттями:

- автентифікація;
- обліковий запис;
- вбудовані ролі сервера.

Кожному користувачу присвоюється обліковий запис з визначеними правами. Автентифікація користувачів проводиться або за обліковим записом на рівні сервера. Паролі користувачів та інші дані про них зберігаються на сервері в системній базі даних. Паролі можуть зберігатися як в зашифрованому, так і в незашифрованому, але спеціально перетвореному вигляді. При інсталяції сервера автоматично створюється обліковий запис системного адміністратора сервера *root*, пароль до якого не можна залишати пустим. Облікові записи користувачів поділяються на адміністративні та користувацькі.

Роль адміністратора бази даних має абсолютні права у СКБД MySql:

- права по керуванню зв'язаними серверами, конфігуруванню процедур, що зберігаються, які запускаються на старті сервера;

- право на зупинку сервера, зміну параметрів роботи служб, застосування змін, керування повнотекстовим пошуком;
- можливість створювати нові облікові записи, надавати їм права на створення БД та їх об'єктів, керувати зв'язаними серверами;
- право створювати нові БД, видаляти або перейменовувати вже існуючі, відновлювати БД з резервних копій;
- право вставляти дані з допомогою засобів масової закладки без безпосереднього доступу до таблиць.

У сервері MySQL автоматично створюється користувач:

- Адміністратор БД має абсолютні права з керування нею. За замовчуванням у користувача відображається обліковий запис *root*, якому тим самим надаються максимальні права в базі даних.

Для вирішення стандартних задач з розмежування прав доступу використовуються фіксовані ролі БД. Крім того в КЗЗ сервера БД реалізовано можливість створювати роль користувача із заданими правами.

2.3.1 Права доступу, що реалізуються штатним КЗЗ

Усі існуючі в БД права доступу розбиваються на три класи:

- права доступу до даних;
- права на виконання процедур, що зберігаються;
- права на виконання команд SQL.

2.3.1.1 Права доступу до даних

Право «INSERT» дозволяє вставляти в таблицю або в подання. Як наслідок, право INSERT може бути видано тільки на рівні таблиці або подання, і не може бути надане на рівні стовпця.

Право «UPDATE» видається або на рівні таблиці, або на рівні стовпця.

Право «DELETE» дозволяє видаляти рядки з таблиці або подання. Як і право INSERT, право DELETE може бути видано тільки на рівні таблиці або подання і не може бути видано на рівні стовпця.

Право «SELECT» дозволяє здійснювати вибірку даних. Може видаватися як на рівні таблиці, так і на рівні окремого стовпця.

2.3.1.2 Права на виконання процедур і функцій, що зберігаються

Єдине право доступу, яке може бути надано відносно процедури, що зберігається - це право на її виконання (CALL). Крім того, власнику процедури, що зберігається, дозволяється продивлятися та змінювати її код.

2.3.1.3 Права на виконання команд SQL.

Права на виконання команд SQL призначено для керування можливостями користувача створювати нові об'єкти БД.

Право "CREATE DATABASE" дозволяє створювати бази даних.

Право "CREATE TABLE" дозволяє створювати таблиці.

Право "CREATE VIEW" дозволяє створювати подання.

Право "CREATE PROCEDURE" дозволяє створювати процедури, що зберігаються.

Право "CREATE FUNCTION" дозволяє створювати функції користувачів.

Право "ALL" надає можливість користуватися усіма вище переліченими правами.

Адміністратор БД автоматично має право ALL. Члени інших облікових записів мають набір прав, відповідно до функцій ролі.

2.3.2 Інші засоби штатних КЗЗ сервера БД

До інших засобів штатних КЗЗ сервера БД слід віднести:

- шифрування об'єктів БД;
- заборона доступу до об'єктів БД;
- засоби аудиту.

Додатковим засобом захисту інформації є використання вбудованих засобів шифрування об'єктів БД. Щоб зашифрувати об'єкт, при його створенні необхідно вказати опцію "ENCRYPTION".

Штатні КЗЗ сервера БД дозволяють встановлювати два типи заборони доступу: явна та неявна. Різниця між ними в тому, що у разі явної заборони користувач не отримає доступу до об'єкту БД ні за яких умов. За неявної заборони користувач може отримати доступ до об'єкту БД. Наприклад у випадку, якщо користувач має неявну заборону на доступ, але його ролі надано явний дозвіл, то він отримає доступ. І навпаки, якщо ролі користувача неявно заборонено доступ, але користувач має явний дозвіл, то він також отримає доступ до об'єкту БД.

2.4 КЗЗ HTTP-сервера Apache

У КЗІ в якості веб-сервера використовується Apache.

2.4.1 Категорії інформації, що обробляється веб-сервером.

Інформація, що обробляється веб-сервером: технологічна інформація.

До технологічної інформації веб-серверу відноситься технологічна інформація КЗІ та технологічна інформація щодо адміністрування та управління обчислювальною системою і засобами обробки інформації - дані щодо мережевих адрес, імен, персональних ідентифікаторів та паролів користувачів, їхні повноваження та права доступу до об'єктів, інформація журналів реєстрації дій користувачів, інша інформація баз даних захисту, встановлені робочі параметри окремих механізмів або засобів захисту, інформація щодо профілів обладнання та режимів його функціонування, робочі параметри функціонального ПЗ тощо.

Технологічна інформація призначена для використання тільки уповноваженими користувачами з числа співробітників ДП "ЕНЕРГОРИНОК" та персоналу, що забезпечує функціонування ЦСК.

2.4.2 Методи обробки інформації веб-сервера

У Apache реалізовано перевірку вмісту запитів, що надходять. При надходженні запиту на статичну html-сторінку (сторінку, яка міститься в html-файлі), веб-сервер надсилає відповідний файл користувачеві, при надходженні запиту на динамічну сторінку (яка формується за запитом користувача) - запускає скрипт і передає йому запит на обробку. Скрипт може бути написано мовами PHP, Perl, ASP тощо.

Результати обробки повертаються користувачу як динамічно згенерована html-сторінка і (необов'язково) зберігаються на сервері. У цьому випадку користувач може змінювати вміст сторінок відповідно до своїх повноважень. У цьому випадку відповідальність за контроль повноважень користувача і коректну обробку даних запиту покладається на скрипт обробки.

Усі механізми захисту, описані нижче, використовуються лише при роботі з користувачами по мережі і відносяться до статичних html-сторінок.

Специфікації механізмів захисту містять описи функцій безпеки.

2.4.3 Основні функції штатного КЗЗ веб-сервера

Основними функціями штатного КЗЗ є: керування доступом до ресурсів веб-сервера на основі облікових записів та груп;

- аудит подій безпеки;
- мінімізація привілеїв;
- захист цілісності конфігураційних файлів;
- контроль використання ресурсів;
- ідентифікація та автентифікація при обміні.

2.4.3.1 Керування доступом до ресурсів веб-сервера на основі облікових записів та груп

Веб-сервер Apache має свою систему облікових записів, незалежну від облікових записів ОС, під керуванням якої він працює. Облікові записи ОС використовуються для контролю доступу до командного інтерпретатора ОС, тоді як облікові записи Apache використовуються для обмеження доступу до певних веб-сторінок.

Функція керування обліковими даними забезпечує безпечне збереження облікових даних користувача. Облікові дані користувача зберігаються у захищеному файлі в текстовому вигляді. При цьому використовується такий формат запису: послідовно записані ім'я користувача і геш - значення паролю.

Облікові записи Apache і дозволи, пов'язані з ними, використовуються лише при запиті веб-сторінки по мережі. Надання або заборона конкретного виду доступу здійснюється на основі зіставлення імені

користувача і правил доступу до захищеного об'єкту, що записані у файлі `.htaccess`. Доступ до захищеного об'єкту надається системою лише у разі, якщо в файлі `.htaccess` вказано відповідне правило доступу для користувача.

Файл має текстовий формат, який може бути відредаговано засобами ОС. Формат файлу `.htaccess`.

Система облікових записів Apache підтримує об'єднання користувачів у групи. Назва файлу з групами задається директивою `AuthGroupFile` в файлі `.htaccess`. Існує одна вбудована група `ALL` - тобто всі користувачі. Права доступу для груп встановлюються таким же чином, як і для користувачів. Файл з групами має текстовий формат, в якому просто перелічені групи та їх склад.

2.4.3.2 Аудит подій безпеки

У штатному КЗЗ веб-сервера реалізовано набір засобів аудиту, що призначені для моніторингу та виявлення небажаних умов і подій, які виникають в обчислювальному середовищі.

Моніторинг системних подій дозволяє виявляти порушників системи безпеки. Аудит дозволяє вести моніторинг конкретних подій.

Перегляд журналу безпеки здійснюється за допомогою стандартних засобів ОС для перегляду файлів. Журнали безпеки зберігаються у текстових файлах, що розміщуються у захищеному каталозі `/var/log/`. Доступ до файлів та каталогу дозволено лише членам групи адміністраторів ОС із застосуванням засобів розмежування доступу ОС.

Політика аудиту задається у текстовому файлі `/usr/local/httpd.conf` і дозволяє визначати перелік подій, для яких повинен проводитися аудит. Для включення можливості ведення аудиту необхідно підключити модуль `config_log_module` та внести відповідні налаштування (перелік подій, що відслідковуються, і формат представлення результатів) в `httpd.conf`. Веб-сервер при запуску перевіряє правильність файлу `httpd.conf`, та у випадку виявлення не коректності видає адміністраторові відповідне попередження.

2.4.3.3 Мінімізація привілеїв

При отриманні запиту на з'єднання головний процес Apache створює дочірній процес з правами користувача `nobody`, для якого в ОС встановлено мінімально можливий набір прав. Цьому процесу і передається обробка з'єднання. Для кожного запиту на з'єднання створюється окремий дочірній процес, тому у випадку успішної атаки зловмисник отримає права `nobody` і не зможе ніяким чином зашкодити ні ОС, ні з'єднанням інших користувачів, які обробляються іншими копіями процесу.

2.4.3.4 Захист цілісності конфігураційних файлів

Apache має вбудовані засоби контролю конфігураційних файлів. У випадку виявлення синтаксичних помилок у конфігураційних файлах (`.htaccess` та `httpd.conf`) Apache видасть повідомлення про помилку і продовжить виконання з правильними значеннями параметрів конфігурації. Перечитування і контроль відбуваються при запуску (перезапуску) веб-сервера Apache або після команди на перечитування конфігурації. Такий механізм дозволяє виявити помилки адміністратора.

При спробі доступу до файлів, доступ до яких заборонено в файлі `.htaccess`, веб-сервер поверне код помилки `403 Forbidden` (доступ заборонено).

2.4.3.5 Контроль використання ресурсів

Механізми контролю використання ресурсів включають такі логічно відокремлені функціональні компоненти:

- контроль кількості одночасних з'єднань, що обробляються;
- контроль кількості одночасно відкритих файлів;
- контроль кількості оперативної пам'яті, що виділяється для обробки з'єднань;
- контроль кількості процесорного часу.

Apache містить засоби обмеження на кількість одночасно оброблюваних з'єднань. У файлі конфігурації `httpd.conf` наявний параметр `MaxClients`, який обмежує максимальну кількість одночасно оброблюваних з'єднань. Стандартне значення 150 рекомендоване для більшості серверів. Один дочірній процес Apache займає в пам'яті приблизно 21 Мб. Існує можливість розрахувати більш точне значення параметру `MaxClients` виходячи з наявного обсягу вільної оперативної пам'яті.

Усі дочірні процеси Apache працюють від імені користувача `nobody`, для якого засобами ОС встановлюється обмеження на максимальну кількість одночасно відкритих файлів. Налаштування цього параметру проводиться в текстовому файлі `/etc/login.conf` зміною значення параметра `openfiles`.

Усі дочірні процеси Apache працюють від імені користувача `nobody`, для якого засобами ОС встановлюється обмеження на максимальну кількість оперативної пам'яті, яка виділяється для обробки

з'єднань. Налаштування цього параметру проводиться в текстовому файлі `/etc/login.conf` зміною значення параметра `memoryuse`.

Усі дочірні процеси Apache працюють від імені користувача `nobody`, для якого засобами ОС встановлюється обмеження на максимальну кількість процесорного часу. Налаштування цього параметру проводиться в текстовому файлі `/etc/login.conf` зміною значення параметра `cputime`.

2.4.3.6 Ідентифікація та автентифікація при обміні

Обмін між компонентами ЦСК здійснюється за протоколом `http` поверх протоколу управління передачею `TCP` з підтвердженням прийому даних, механізми якого реалізують функції ідентифікації і автентифікації між K33 відправника та K33 одержувача на підставі їх імен та/або IP-адреси.

Для обмеження доступу за IP-адресою до файлів певного каталогу у ньому необхідно створити файл `.htaccess` з переліком правил доступу. Можливе також обмеження доступу для конкретного користувача.

При обмеженні доступу за іменем користувача можливе використання двох типів автентифікації: `"basic"` та `"digest"`.

При використанні автентифікації `"basic"` пароль користувача передається у відкритому вигляді. Тому такий тип автентифікації є небезпечним.

При використанні автентифікації `"digest"` пароль користувача передається у вигляді геш-значення за спеціальним протоколом з використанням випадкових даних, що унеможливує відновлення пароля або повторне використання перехоплених даних автентифікації. Отже такий тип автентифікації є безпечнішим.

2.5 Підсистема антивірусного захисту

У якості засобу антивірусного захисту використовується "ESET Endpoint Antivirus". Програмний засіб антивірусного захисту має чинний, позитивний експертний висновок Адміністрації Держспецзв'язку України у сфері ТЗІ.

Засоби антивірусного захисту реалізують такі функції:

- застосування евристичних методів захисту у процесі викриття шкідливого ПЗ;
- захист файлової системи;
- оновлення антивірусних баз.

2.5.1 Застосування евристичних методів захисту у процесі викриття шкідливого ПЗ

Застосування евристичних методів захисту дозволяє забезпечити захист від шкідливого ПЗ, опис яких ще відсутній у базі. Методи ґрунтуються на аналізі процесів запущених у ОС та дозволяють попередити користувача про можливу небезпеку та запобігти їй.

Евристичний аналіз ґрунтується на (вельми правдоподібному) припущенні, що нові віруси часто виявляються схожі на які-небудь з вже відомих. Таке припущення виправдовується наявністю в антивірусних базах сигнатур для визначення не одного, а відразу декількох вірусів. Заснований на такому припущенні евристичний метод полягає в пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів.

Позитивним ефектом від використання цього методу є можливість виявити нові віруси ще до того, як для них будуть виділені сигнатури.

2.5.2 Захист файлової системи

Захист файлової системи базується на тому, що САЗ РС здійснює антивірусну перевірку усіх файлів під час їх створення, запуску або модифікації. Реалізована можливість перевірки окремих файлів, каталогів, дисків (локальних, мережевих).

Антивірус захищає файлові сховища в режимі реального часу, видаляючи віруси, троянські та інші шкідливі програми.

За замовчуванням антивірус перевіряє тільки нові або змінені файли, тобто файли, які додалися або змінилися з часу останнього звернення до них. Процес перевірки файлу виконується за наступним алгоритмом:

- звернення користувача або деякої програми до кожного файлу перехоплюється компонентом;
- антивірус перевіряє наявність інформації про перехоплений файл у антивірусних базах. На підставі отриманої інформації приймається рішення про необхідність перевірки файлу.

Спочатку файл аналізується на присутність вірусів. Розпізнавання шкідливих об'єктів відбувається на підставі баз вірусів програми. Бази містять опис всіх відомих на даний момент шкідливих програм, погроз, мережних атак і способів їх знешкодження.

В результаті аналізу можливі наступні варіанти поведінки програми: якщо у файлі виявлено шкідливий код, антивірус блокує файл і намагається її лікувати. В результаті успішного лікування файл стає доступним для роботи. Якщо лікування провести не вдалося, файл видаляється. При виконанні лікування файлу або його видаленні копія файлу поміщається в резервне сховище.

Якщо у файлі виявлено код, схожий на шкідливий, але стовідсоткової гарантії цього немає, файл поміщається в спеціальне сховище - карантин. Пізніше можна спробувати вилікувати його з оновленими базами.

Якщо у файлі не виявлено шкідливого коду, він відразу ж стає доступним для роботи.

2.5.3 Оновлення антивірусних баз

Антивірус виконує пошук шкідливих програм і лікування заражених об'єктів на підставі записів антивірусних баз. Вкрай важливо підтримувати антивірусні бази в актуальному стані, оскільки щодня з'являються нові віруси, троянські та інші шкідливі програми.

Оновлення антивірусних баз відбувається одразу після інсталяції антивірусного засобу. За замовчанням процедура оновлення проходить у автоматичному режимі при належності на комп'ютері з'єднання з Інтернетом. Тому, для коректної роботи антивірусу і автоматичного оновлення антивірусних баз необхідно налагодити безперешкодний доступ до мережі Інтернет антивірусному програмному забезпеченню.

2.6 КЗЗ операційної системи з лінійки Linux для серверів

У якості ОС серверів взаємодії використовуються ОС з лінійки Linux - дистрибутив FreeBSD 9.2.

КЗЗ ОС реалізує такі функції:

- забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК, що зберігаються у файлової системі;
- забезпечення безперервності функціонування ОС;
- ведення журналів аудиту;
- забезпечення можливості адміністрування, керування і підтримки ОС.

2.6.1 Забезпечення захисту від несанкціонованого доступу (НСД) до об'єктів захисту ЦСК

Операційна система (ОС) надає доступ до своїх ресурсів тільки авторизованим користувачам. Список доступу включає перелік користувачів, яким дозволено доступ до об'єкта, а також набір дозволених над об'єктом дій, що у явному вигляді є елементами захисту від НСД.

Для спрощення керуванням доступом до об'єктів і захисту від НСД, ОС дозволяє створювати групи безпеки, дозволяючи призначати дозволи і права для групи користувачів, а не окремому обліковому запису користувача. Для надання доступу до ресурсів, обліковий запис може бути добавлений або видалений з групи користувачів. Після інсталяції ОС в ньому створюються вбудовані групи, які дають право на виконання напередвизначених системних завдань.

2.6.2 Забезпечення безперервності функціонування ОС

Важливим, а іноді необхідним для роботи ОС є забезпечення безперервності функціонування. Невиконання цієї умови може привести до втрати важливої інформації. Головними умовами безперервного функціонування є використання журналюємої файлової системи.

Журналюєма файлова система дозволяє забезпечити транзакційність запису даних за рахунок формування журналу дій перед здійсненням запису.

У випадку збоїв драйвер ОС аналізує журнал файлової системи і або завершує транзакцію, або повертає файлову систему у попередній стан.

2.1.3 Ведення журналів аудиту

У ОС присутній набір засобів аудиту, призначених для моніторингу та виявлення умов і подій що пов'язані з можливим НСД або є небажаними, які виникають в обчислювальному середовищі. Моніторинг системних подій дозволяє виявляти порушників, що здійснюють спроби НСД, а також фіксувати спроби НСД з метою фальсифікації та видалення даних, які знаходяться на локальному комп'ютері.

При аудиті, частіше за все, реєструються такі події як доступ до об'єктів, керування групами користувачів і обліковими записами груп, а також вхід користувачів в систему і вихід з неї. Аудит дозволяє вести моніторинг конкретних подій, наприклад, неуспішних спроб входу до системи. Перегляд журналу безпеки виконується за допомогою засобів перегляду подій. Політика аудиту дозволяє визначати події, для яких повинен проводитися аудит.

2.1.4 Забезпечення можливості адміністрування, керування і підтримки ОС

Операційна система Linux (дистрибутив FreeBSD зокрема) володіє багатьма можливостями адміністрування, керування та підтримки. Системи адміністрування надають можливість керувати файловою системою, установкою та видаленням програмного забезпечення, налаштування журналів безпеки та багато інших.

Налаштування усіх програм та служб ОС зберігаються у конфігураційних файлах у каталозі /etc у легке внесення налаштувань з використанням лише текстового редактора.

ОС надає можливість віддаленого керування ОС спільно з іншим користувачем, комп'ютер якого підключений до мережі.

З дозволу користувача, ОС завантажує критично важливі оновлення з Інтернету в фоновому режимі. Завантаження не потребує від користувача додаткових зусиль або переривання в роботі.